



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/816,687

04/02/2004

Uwe Eckhardt

5800-00601

9738

53806

7590

06/06/2008

MEYERTONS, HOOD, KIVLIN, KOWERT & GOETZEL (AMD)

P.O. BOX 398

AUSTIN, TX 78767-0398

EXAMINER

SAN JUAN, MARTINJERIKO P

ART UNIT

PAPER NUMBER

2132

MAIL DATE

DELIVERY MODE

06/06/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/816,687	Applicant(s) ECKHARDT ET AL.	
	Examiner MARTIN JERIKO P. SAN JUAN	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 25 April 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-3,6-69 and 71-73 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-3,6-69 and 71-73 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 02 April 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

This is a response to Applicant's Remarks filed on April 25, 2008.

Claims 1-3, 6-69, and 71-73 are currently pending.

Response to Arguments

1. Applicant's arguments filed on April 25, 2008 have been fully considered but they are not persuasive.

Beach teaches or suggests data frame encapsulation/decapsulation based on conforming with the IEEE 802.11 standard. IEEE 802.11 discloses data frame encapsulation/decapsulation as it describes how MAC frames should be constructed in Chapter 7 of the IEEE 802.11 standard (1999 edition). Beach conforming with the IEEE 802.11 and disclosing all MAC processing functions in [Beach 4: 0042-0063] teaches or suggests data frame encapsulation/decapsulation. Beach embodiment in Figure 2 is the same architecture of the Applicant as described in the Specification Figure 5. Beach disclosing that all MAC processing functions, except roaming/association controls, be on the MAC engine teaches or suggests that data frame encapsulation/decapsulation also be in the MAC engine because data frame encapsulation/decapsulation is part of constructing data MSDUs. Beach teaches the feasibility of having the described above MAC processing/functions in a single-purpose hardware, called the MAC engine DSP processor in Par 0111-0114. Beach intends a MAC engine DSP processor not to involve software-implemented instructions of a driver

software that enables the host processor and host resources to execute the MAC processing functions [Par 0111].

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

1. Claims 1-3, 6-13, 16-20; 26-27, 30-31, 46-61,69, and 71-73 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beach [US 2001/0055283 A1], and further in view of Edwards et al. [US 2004/0059825 A1], hereinafter Edwards.

Regarding claim 1, Beach teaches a method of performing encrypted WLAN (Wireless Local Area Network) communication, comprising the steps of: operating driver software to perform a connection set-up for said encrypted WLAN communication [US 2001/0055283 A1, Pg 4, Par 0054-0058] [US 2001/0055283 A1, Pg 7, Par 0110]; and operating a WLAN chip to perform data frame encapsulation and/or decapsulation during said encrypted WLAN communication [US 2001/0055283 A1, Pg 4, Par 0060-0062] [US 2001/0055283 A1, Pg 7, Par 0110]; wherein said connection set-up is performed by executing software-implemented instructions of said driver software without exchanging intermediate data with said WLAN chip [US 2001/0055283 A1, Pg 4, Par 0054-0058] [US 2001/0055283 A1, Pg 7-8, Par 0111]; and wherein said data frame encapsulation and/or decapsulation is performed by operating single-purpose hardware of said WLAN chip without executing software-implemented instructions of said driver software [US 2001/0055283 A1, Pg 4, Par 0059] [US 2001/0055283 A1, Pg

3-4, Par 0037] [US 2001/0055283 A1, Pg 7, Par 0111 --Examiner notes evidence of the partition between hardware and software in terms of the locations of the various MAC functions.]

However, Beach does not explicitly teach wherein performing said connection set-up comprises exchanging cryptographic keys between a WLAN station and another WLAN station and/or a WLAN access point, and wherein performing said encrypted WLAN communication further comprises obtaining a plurality of data frames intended for said data frame encapsulation from driver software.

Edwards teach performing said connection set-up comprises exchanging cryptographic keys between a WLAN station and another WLAN station and/or a WLAN access point [US 2004/0059825 A1, Pg 2, Par 0012] [US 2004/0059825, Pg 6, Par 0059] and wherein performing said encrypted WLAN communication further comprises obtaining a plurality of data frames intended for said data frame encapsulation from driver software [US 2004/0059825, Pg 5, Par 0050].

It would have been obvious to one of ordinary skilled in the art at the time of invention to implement Edward's hardware/software partition functionality into Beach's invention.

The suggestion/motivation for combining would have been to add more detail and explicit implementation of the hardware/software partition functionality to balance function and performance centering on timing requirements [US 2004/0059825 A1].

Edwards is an analogous art because it is in the same field of endeavor of designing WLAN cards.

With regard to dependent claim 2, Beach and Edwards teach the method of claim 1,

Art Unit: 2132

wherein the step of performing said connection set-up comprises authenticating a WLAN station by another WLAN station and/or a WLAN authentication server [US 2001/0055283 A1, Pg 10, Par 0138] [WLAN station authentication is inherent as cited for the provision of multiple ESS LANs with three levels of wireless network security]

With regard to dependent claim 3, Beach and Edwards teach the method of claim 1, wherein the step of performing said connection set-up comprises associating a WLAN station with another WLAN station and/or a WLAN access point as WLAN communication counter-parts [US 2001/0055283 A1, Pg 4, Par 0054].

With regard to dependent claim 6, Beach and Edwards teach the method of claim 1, wherein the step of obtaining the plurality of data frames comprises obtaining a plurality of data frames comprising cipher information indicating a determining factor for performing the data frame encapsulation and/or decapsulation [US 2001/0055283 A1, g 9, Par 0131-0134].

With regard to dependent claim 7, Beach and Edwards teach the method of claim 6, therein said determining factor comprises a way in which a data frame intended for the data frame encapsulation is fragmented [US 2001/0055283 A1, Pg 9, Par 0133].

With regard to dependent claim 8, Beach and Edwards teach the method of claim 6, wherein said determining factor comprises a cipher protocol suitable for performing the data frame encapsulation [US 2001/0055283 A1, Pg 8, Par 0122] [WEP is the cipher protocol as cited.].

With regard to dependent claim 9, Beach and Edwards teach the method of claim 6, wherein said determining factor comprises a cryptographic key suitable for encrypting a

data frame [US 2001/0055283 A1, Pg 6, Par 0094].

With regard to dependent claim 10, Beach and Edwards teach the method of claim 1, wherein performing said encrypted WLAN communication further comprises selecting one of the plurality of data frames for said data frame encapsulation by performing a prioritization algorithm implemented on the single-purpose hardware [US 2001/0055283 A1, Pg 10; Par 0139].

With regard to dependent claim 11, Beach and Edwards teach the method of claim 1, wherein the step of performing said data frame encapsulation comprises inserting a package number and/or sequence number into one of the plurality of data frames [US 2001/0055283 A1, Pg 9, Par 0131-0134] [This is inherent in the frame control field using the IEEE 802.11 standard (Brenner, 1997, Pg 19)].

With regard to dependent claim 12, Beach and Edwards teach the method of claim 1, wherein the step of performing said data frame encapsulation comprises encrypting at least part of one of the plurality of data frames [US 2001/0055283 A1, Pg 8, Par 0122].

With regard to dependent claim 13, Beach and Edwards teach the method of claim 1, wherein the step of performing said data frame encapsulation comprises calculating an integrity value appropriate for verifying integrity of one of the plurality of data frames once said data frame decapsulation is completed [US 2001/0055283 A1, Pg 9, Par 0132].

With regard to dependent claim 16, Beach and Edwards teach the method of claim 1, wherein performing said encrypted WLAN communication further comprises receiving a data frame intended for said data frame decapsulation from a WLAN station and/or

WLAN access point [US 2001/0055283 A1, Pg 3, Par 0036].

With regard to dependent claim 17, Beach and Edwards teach the method of claim 1, wherein the step of performing said data frame decapsulation comprises obtaining cipher information indicating a determining factor for performing the data frame encapsulation and/or decapsulation from a storage unit within the single-purpose hardware [US 2001/0055283 A1, Pg 8, Par 0122].

With regard to dependent claim 18, Beach and Edwards teach the method of claim 17, wherein said determining factor comprises a cipher protocol suitable for performing the data frame decapsulation [US 2001/0055283 A1, Pg 8, Par 0122] [WEP is the cipher protocol as cited.].

With regard to dependent claim 19, Beach and Edwards teach the method of claim 17, wherein said determining factor comprises a cryptographic key suitable for decrypting a data frame [US 2001/0055283 A1, Pg 6, Par 0094].

With regard to dependent claim 20, Beach and Edwards teach the method of claim 16, wherein the step of performing said data frame decapsulation comprises decrypting at least part of the data frame [US 2001/0055283 A1, Pg 8, Par 0122].

With regard to dependent claim 26, Beach and Edwards teach the method of claim 1, wherein the step of performing said data frame encapsulation and/or decapsulation comprises generating cryptographic data suitable for encrypting or decrypting a data frame [US 2001/0055283 A1, Pg 6, Par 0094].

With regard to dependent claim 27, Beach and Edwards teach the method of claim 26, wherein the step of generating cryptographic data comprises generating authentication

data suitable for encrypting a data frame in a manner specific to a WLAN station or decrypting a data frame encrypted in a manner specific to a WLAN station [US 2001/0055283 A1, Pg 6, Par 0094] [US 2001/0055283 A1, Pg 10, Par 0138-0139] [Generating said authentication data specific to a WLAN station is inherent for the application of providing multiple ESS LANs with multiple levels of security of wireless networks whereby the cell controller can perform the function of determining which ESS network a mobile unit is communicating with an RF port associated with the cell controller is operating on and verifying the multiple levels of security provided in connection with the access by the mobile unit devices as cited.].

With regard to dependent claim 30, Beach and Edwards teach the method of claim 1, wherein said software-implemented instructions are executed on general-purpose hardware by driver software [US 2001/0055283 A1, Pg 5, Par 0065].

With regard to dependent claim 31, Beach and Edwards teach the method of claim 1, wherein said single-purpose hardware is operated periodically [US 2001/0055283 A1, Pg 7, Par 0101].

Independent claims 46, 69, and 71 are simply the entities for performing the method of claim 1. Claim 46 is a single-purpose hardware device; 69 is an integrated circuit chip; 71 is a computer system all performing the same method of claim 1.

Claims 46, 69, and 71 are rejected using the same references as claim 1.

With regard to dependent claim 47, Beach and Edwards teach the single-purpose hardware device of claim 46, wherein said internal hardware components further comprise internal memory for storing data frames intended for or resulting from the

Art Unit: 2132

data frame encapsulation or decapsulation [US 2001/0055283 A1, Pg 9, Par 0131-0134] [US 2001/0055283 A1, Pg 5, Par 0071] [US 2001/0055283 A1, Pg 5, Par 0074-0075] [US 2004/0059825 A1, Fig 8, Itms 36, 38, 48].

With regard to dependent claim 48, Beach and Edwards teach the single-purpose hardware device of claim 47, wherein said internal memory comprises an arbitration unit for performing memory access control [US 2001/0055283 A1, Pg 5, Par 0079].

With regard to dependent claim 49, Beach and Edwards teach the single-purpose hardware device of claim 47, wherein said internal memory comprises a hash memory for storing cipher information indicating a determining factor for performing the data frame encapsulation and/or decapsulation [US 2001/0055283 A1, Pg 9, Par 0131-0134] [US 2001/0055283 A1, Pg 5, Par 0071] [US 2001/0055283 A1, Pg 5, Par 0074-0075] [US 2004/0059825 A1, Fig 8, Itms 36, 38, 48].

With regard to dependent claim 50, Beach and Edwards teach the single-purpose hardware device of claim 49, wherein said determining factor comprises a cipher protocol suitable for performing the data frame encapsulation and/or decapsulation [US 2001/0055283 A1 , Pg 8, Par 0122] [WEP is the cipher protocol as cited.].

With regard to dependent claim 51, Beach and Edwards teach the single-purpose hardware device of claim 49, wherein said determining factor comprises a cryptographic key suitable for encrypting or decrypting a data frame [US 2001/0055283 A1, Pg 6, Par 0094].

With regard to dependent claim 52, Beach and Edwards teach the single-purpose hardware device of claim 47, wherein said internal hardware components further

Art Unit: 2132

comprise a radio transceiver for receiving data frames from and/or transmitting data frames to a WLAN station and/or WLAN access point [US 2001/0055283 A1, Pg 5, Par 0071].

With regard to dependent claim 53, Beach and Edwards teach the single-purpose hardware device claim 52, wherein said internal single-purpose hardware components comprise a cryptographic component for performing the data frame encapsulation and/or decapsulation and a MAC (Medium Access Control) component for communicating with the radio transceiver [US 2001/0055283 A1, Pg 5, Par 0072] [US 2001/0055283 A1, Pg 6, Par 0093].

With regard to dependent claim 54-57, it is inherent that Beach and Edwards teach: the cryptographic component and internal memory are arranged to communicate with each other; cryptographic component and MAC component are arranged to communicate with each other; MAC component and internal memory are arranged to communicate with each other; and internal memory is arranged to communicate over the interface with external hardware components.

With regard to dependent claim 58, Beach and Edwards teach the single-purpose hardware device of claim 53, wherein said MAC component further is for performing a prioritization algorithm for selecting a data frame for said data frame encapsulation from a plurality of data frames [US 2001/0055283 A1, Pg 10, Par 0139] [US 2004/0059825 A1, Pg 5, Par 0052].

Dependent claims 59-61 are rejected using the same references as claims 11, 26, and 27 respectively. Claims 59-61 is the apparatus for performing the method claims of 11,

Art Unit: 2132

26, and 27 respectively.

Regarding claim 72, Beach and Edwards teach the method as recited in claim 1, wherein the single-purpose hardware is a circuit dedicated for performing encapsulation and decapsulation without execution of any software instructions [US 2004/0059825, Fig 4] [US 2004/0059825 A1, Pg 4, Par 0050].

Regarding claim 73, Beach and Edwards teach the method as recited in claim 72, wherein the single-purpose hardware is coupled to receive plaintext data from the driver software, and wherein the single-purpose hardware is further coupled to provide decapsulated data to the driver software [US 2004/0059825, Fig 4] [US 2004/0059825 A1, Pg 4, Par 0050 -Examiner notes "unprocessed/raw packets" reading on plaintext data.].

2. Claims 14-15, 21-25, 28-29, 32-35, 39-45, 62, and 65-68 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beach [US 2001/0055283 A1], Edwards et al. [US 2004/0059825 A1], hereinafter Edwards, and further in view of Park [US 2004/0146158 A1].

With regard to dependent claim 14, Beach and Edwards teach the method of claim 13. However, Beach and Edwards do not teach wherein the step of performing said data frame encapsulation comprises encrypting said integrity value.

Park teaches wherein the step of performing said data frame encapsulation comprises encrypting said integrity value [US 2004/0146158 A1, Pg 1, Par 0005].

It would have been obvious to one of ordinary skill in the art to modify Beach and Edwards to combine the methods of Park's cryptographic systems that support multiple

Art Unit: 2132

modes of operation. The suggestion/motivation for combining would have been to include provisions for confidentiality, integrity, and origin authentication of messages [US 2004/0146158 A1, Pg 1, Par 0003-0004]. Park is an analogous art because it is in the same field of performing secure communications in a wireless local area network.

With regard to dependent claim 15, Beach, Edwards, and Park teach the method of claim 14, wherein the step of performing said data frame encapsulation comprises inserting the encrypted integrity value into one of the plurality of data frames [US 2004/0146158 A1, Pg 1, Par 0004 -Examiner notes this limitation to be inherent in IEEE 802.11i.].

With regard to dependent claim 21, Beach, Edwards, and Park teach the method of claim 20, Wherein the data frame comprises an encrypted integrity value appropriate for verifying integrity of the data frame once said data frame decapsulation is completed, and the step of decrypting at least part of the data frame comprises decrypting the encrypted integrity value [US 2004/0146158 A1, Pg 1, Par 0006].

With regard to dependent claim 22, Beach, Edwards, and Park teach the method of claim 21, wherein the step of performing said data frame decapsulation further comprises calculating the integrity value from at least part of the data frame except the encrypted integrity value [US 2004/0146158 A1, Pg 1, Par 0006].

With regard to dependent claim 23, Beach, Edwards, and Park teach the method of claim 22, wherein the step of performing said data frame decapsulation further comprises calculating an integrity verification value indicating a difference between the decrypted integrity value and the calculated integrity value [US 2004/0146158 A1, Pg 1,

Art Unit: 2132

Par 0006 --Examiner notes calculating an integrity verification value indicating a difference between the decrypted integrity value and the calculated integrity value is evident when comparing values.].

With regard to dependent claim 24, Beach, Edwards, and Park teach the method of claim 23, wherein the step of performing said data frame decapsulation further comprises inserting said integrity verification value into the data frame frames [US 2004/0146158 A1, Pg 1, Par 0004 -Examiner notes this limitation to be inherent in IEEE 802.11i.].

With regard to dependent claim 25, Beach, Edwards, and Park teach the method of claim 24, wherein performing said encrypted WLAN communication further comprises performing counter-measures according to said integrity verification value by executing software-implemented instructions, wherein said counter-measures are suitable for limiting the amount of information available to an illegitimate WLAN protruder frames [US 2004/0146158 A1, Pg 1, Par 0004 -Examiner notes this limitation to be inherent in IEEE 802.11i.].

With regard to dependent claim 28, Beach, Edwards, and Park teach the method of claim 1, wherein said encrypted WLAN communication is performed based on the IEEE 802.11i security standard [US 2004/0146158, Pg 1, Par 0004].

With regard to dependent claim 29, Beach, Edwards, and Park teaches the method of claim 1. However Beach and Park doesnot explicitly teach wherein said encrypted WLAN communication is performed in a WLAN based on the IEEE 802.11b standard. It would have been obvious to perform a WLAN based on the IEEE802.11b to

Art Unit: 2132

accommodate higher data throughput when already implementing the IEEE 802.11 Standard [US 2001/0055283 A1, Pg 1, Par 0003].

With regard to dependent claim 32, Beach, Edwards, and Park teaches the method of claim 31. However Beach and Park does not explicitly teach wherein said single-purpose hardware is operated periodically at 11 MHz.

It would have been obvious to have said single-purpose hardware be operated periodically at 11 MHz, since the single-purpose hardware is driven by either an external crystal or clock [US 2001/0055283 A1, Pg 7, Par 0100].

With regard to dependent claim 33, Beach, Edwards, and Park teach the method of claim 31, wherein said data frame encapsulation and/or decapsulation is performed according to the TKIP (Temporal Key Integrity Protocol) protocol [US 2004/0146158.A1, Pg 1, Par 0004-Examiner notes this limitation to be inherent in IEEE 802.11i].

With regard to dependent claim 34, Beach, Edwards, and Park teach the method of claim 33, wherein the step of performing said data frame encapsulation and/or decapsulation comprises performing RC4 (Rivest's Cipher 4) encryption and/or decryption [Pg 6, Par 0094].

With regard to dependent claim 35, Beach, Edwards, and Park teach the method of claim 34, wherein said RC4 encryption and/or decryption is performed by operating at least part of the single-purpose hardware [Pg 6, Par 0094-0095].

With regard to dependent claim 39, Beach, Edwards, and Park teach the method of claim 34, wherein the step of performing said RC4 encryption and/or decryption comprises encrypting or decrypting at least part of a data frame comprising bytes, and

Art Unit: 2132

said RC4 encryption and/or decryption is split over at least two operating periods of the single-purpose hardware to encrypt or decrypt one byte of the data frame [Pg 6-7, Par 0094-0095] [Beach explains the per byte computation burden for the CRC/WEP tasks, and as cited, an alternative solution to timing issues due to CPU limitations would be to catch up first for the packet CRC calculation and then catch up with WEP/CRC tasks which is essentially splitting over the operations for at least two operating periods of the CPU.]

With regard to dependent claim 40, Beach, Edwards, and Park teach the method of claim 31, wherein said data frame encapsulation-and/or decapsulation is performed according to the CCMP (Counter-mode Cipher block chaining Message authentication code Protocol) protocol [US 2004/0146158, Pg 1, Par 0004].

With regard to dependent claim 41, Beach, Edwards, and Park teach the method of claim 40, wherein the step of performing said data frame encapsulation and/or decapsulation comprises performing CCMP-AES (Advanced Encryption Standard) encryption and/or decryption [US 2004/0146158, Pg 1, Par 0004].

With regard to dependent claim 42, Beach, Edwards, and Park teaches the method of claim 41, wherein the step of performing said CCMP-AES encryption and/or decryption comprises encrypting or decrypting at least part of a data frame comprising bytes, and said CCMP-AES encryption and/or decryption is performed by repeatedly performing a sequence of encryption or decryption steps on said part of the data frame [US 2004/0146158, Pg 2, Par 0026].

With regard to dependent claim 43, Beach, Edwards, and Park teach the method of

Art Unit: 2132

claim 42, wherein the step of performing the sequence of encryption or decryption steps comprises performing byte substitution using a plurality of cryptographic substitution boxes [US 2004/0146158, Pg 1, Par 0004.].

With regard to dependent claim 44, Beach, Edwards, and Park teach the method of claim 43, wherein the step of performing byte substitution on said part of the data frame comprises sequentially performing the byte substitution on a plurality of sub-parts of said part of the data frame [US 2004/0146158 A1, Pg 1, Par 0004 -Examiner notes this limitation to be inherent in IEEE 802.11i.].

With regard to dependent claim 45, Beach, Edwards, and Park teach the method of claim 42, wherein the step of performing the sequence of encryption or decryption steps is split over at least two operating periods of the single-purpose hardware [Pg 6-7, Par 0094-0095] [Beach explains the per byte computation burden for the CRC/WEF tasks, and as cited, an alternative solution to timing issues due to CPU limitations would be to catch up first for the packet CRC calculation and then catch up with WEP/CRC tasks which is essentially splitting over the operations for at least two operating periods of the CPU.].

Dependent claim 62 is rejected using the same references as claims 33-35. Claim 62 is the apparatus for performing the methods of claims 33-35 combined.

Dependent claim 65 is rejected using the same references as claims 31 and 39. Claim 65 is the apparatus for performing the methods of claims 31 and 39 combined.

Dependent claim 66 is rejected using the same references as claims 40-43. Claim 66 is the apparatus for performing the methods of claims 40-43 combined.

Dependent claim 67 is rejected using the same references as claim 44. Claim 67 is the apparatus for performing the method of claim 44.

Dependent claim 68 is rejected using the same references as claims 31 and 45. Claim 68 is the apparatus for performing the methods of claims 31 and 45 combined.

3. Claims 36-38, and 63-65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beach [US 2001/0055283 A1], Edwards et al. [US 2004/0059825 A1] and further in view of Campbell [Non-Patent Literature, November 2000].

With regard to dependent claim 36, it is inherent that the single-purpose hardware will have a form of data structure for the storage and management of data involved in task/process execution. Beach teaches the method of claim 35, but does not explicitly disclose wherein said part of the single-purpose hardware has a tree structure [Tree structure is interpreted as a form of data structure.] Prior Art disclosed in the specification utilizes an ordered array (Figure 2C). Campbell teaches a tree data structure that combines the advantages of searching performance of an ordered arrays, and the efficiency of insertion and deletion of data in a linked list data type structure. Campbell is an analogous art because it solves the problem of how to store and manage data in a digital device.

It would have been obvious to one of ordinary skill in the art at the time of the invention to use the tree data structure of Campbell [a classic data structure well known in the art] for the storage and management of data involved in task/process execution because the tree data structure can be implemented as opposed to the simpler ordered matrix/array type data structure that is normally used. The suggestion/motivation for

Art Unit: 2132

combining would have been to utilize the combined advantages of an ordered array and the efficiency of a linked list type data structure; thereby increasing efficiency and data throughput by minimizing accesses when searching/retrieving data for various functions of the digital device. Therefore, it would have been obvious to combine Beach with Campbell to obtain the invention as specified in claim 36.

Claim 37 is rejected because it is the same method as claim 36, and wherein said RC4 encryption and/or decryption will inherently be performed by operating only a sub-part of the single-purpose hardware corresponding to the tree root, part of the tree leaves and the tree components interconnecting the tree root with said part of the tree leaves.

Claim 38 is rejected because it is the same method of claim 37, and wherein said sub-part of the single-purpose hardware will inherently correspond to the tree root, two of the tree leaves and the tree components interconnecting the tree root with said two of the tree leaves.

Dependent claim 63 is rejected using the same references and rationale as claims 36-37. Claim 63 is the apparatus for performing the methods of claims 36-37 combined.

Dependent claim 64 is rejected using the same reference and rationale as claim 38.

Claim 64 is the apparatus for performing the method of claim 38.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

Art Unit: 2132

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MARTIN JERIKO P. SAN JUAN whose telephone number is (571)272-7875. The examiner can normally be reached on M-F 8:30a - 6:00p EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MJSJ/

Martin Jeriko San Juan
Examiner. Art Unit 2132.

/Gilberto Barron Jr/

Supervisory Patent Examiner, Art Unit 2132